VIDUNDERLIGE NYE RINGER

John Rognes

Innledning

Denne artikkelen er basert på forfatterens foredrag ved Norsk Matematisk Forenings årsmøte 2002, holdt den 20. mars i Oslo.

I kapittel 1 skal vi gi en elementær definisjon av en "vidunderlig ny ring", basert på ideer av Graeme Segal [Se74], Brian Day [Da70], Marcel Bökstedt (ca. 1985) og Manos Lydakis [Ly99]. Andre likeverdige (men mindre elementære) definisjoner ble gitt av Tony Elmendorf, Igor Kriz, Mike Mandell og Peter May i [EKMM97], samt av Mark Hovey, Brooke Shipley og Jeff Smith [HSS00]. Alle disse alternative definisjonene nådde en endelig form kort etter 1995.

Uttrykket "vidunderlig ny ring" ("brave new ring") ble myntet av Friedhelm Waldhausen til et foredrag ved Northwestern University i Evanston i 1988, med referanse til Aldous Huxleys bok "Vidunderlige Nye Verden" ("Brave New World", 1932), som igjen henspeiler på Mirandas utrop: "O, wonder ! How many goodly creatures are there here ! How beauteous mankind is ! O brave new world, that has such people in't !" i William Shakespeares skuespill "Stormen" ("The Tempest", 1611).

I kapittel 2 vil vi redegjøre for noen anvendelser av disse "vidunderlige nye ringene", til så tilsynelatende svært ulike emner som:

- rom av differensiable og kontinuerlige symmetrier av mangfoldigheter av høy dimensjon (i geometrisk topologi),
- strukturer som gir opphav til konforme- eller topologiske felt-teorier for streng-teori (i matematisk fysikk), og
- kongruenser for theta-funksjoner av jevne unimodulære gittere i den aritmetiske teorien for modulære former (i tallteori).

I kapittel 3 vil vi så rekapitulere deler av den klassiske teorien for elliptiske kurver, modulære former og jevne unimodulære gittere, for bl.a. å kunne sammenlikne komplekse (analytiske) modulære former med heltallige (aritmetiske) modulære former, og videre å kunne vise hvordan topologiske modulære former passer inn i denne sammenhengen.

1. Vidunderlige nye ringer

1.1. Algebra og topologi. En ring er en abelsk gruppe utstyrt med en passende multiplikasjon og enhet. En abelsk gruppe kan oppfattes som en $\mathbb{Z}$-modul, der $\mathbb{Z}$ er ringen av hele tall. Likeledes kan en ring oppfattes som en $\mathbb{Z}$-algebra. Vi skal introdusere en generalisering av begrepet "abelsk gruppe", som ofte kalles et spektrum (i algebraisk topologisk forstand), men som her vil kalles en $\mathbb{S}$-modul.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

En vidunderlig ny ring er da en $\mathbb{S}$-modul med en passende multiplikasjon og enhet, dvs. en $\mathbb{S}$-algebra. Her er $\mathbb{S}$ selv en spesielt vidunderlig ny ring, som gjerne kalles sfærespekteret. Vi får følgende ordliste:

Algebra	Topologi
Abelsk gruppe = $\mathbb{Z}$-modul	Spektrum = $\mathbb{S}$-modul
Ring = $\mathbb{Z}$-algebra	Vidunderlig ny ring = $\mathbb{S}$-algebra
Heltallene = $\mathbb{Z}$	Sfærespekteret = $\mathbb{S}$

1.2. Abelske grupper. Vi begynner med å gi en omstendelig beskrivelse av en abelsk gruppe, valgt slik at den lett lar seg generalisere til å definere en $\mathbb{S}$-modul (i avsnitt 1.4). La A være en abelsk gruppe. Til A vil vi assosiere en regel HA (H for homologi) som:

(1) til hvert heltall $n \geq 0$ tilordner mengden $HA(n_+) = A^n$ som består av alle n-tupler $(a_1, \dots, a_n)$ fra A, og
(2) til hver funksjon $f\colon \{0, 1, \dots, m\} \to \{0, 1, \dots, n\}$ med $m, n \geq 0$ og $f(0) = 0$ tilordner funksjonen $HA(f)\colon A^m \to A^n$ som tar $(a_1, \dots, a_m)$ til $(b_1, \dots, b_n)$ der
$$b_j = \sum_{f(i)=j} a_i \,.$$
Summen løper over de $i = 1, \dots, m$ som oppfyller $f(i) = j$, og dannes i den abelske gruppen A.

Vi kan nesten rekonstruere den abelske gruppen A fra regelen HA. Som mengde er $A = A^1$ tilordnet heltallet $n = 1$. Gruppeoperasjonen $A^2 = A \times A \to A$ er tilordnet funksjonen $f\colon \{0, 1, 2\} \to \{0, 1\}$ med $f(0) = 0$ og $f(1) = f(2) = 1$. Det eneste som mangler er gruppe-inversen.

Vi kan tenke på HA som diagrammet av alle mengdene $HA(n_+) = A^n$ for $n \geq 0$, knyttet sammen med alle funksjonene $HA(f)\colon A^m \to A^n$ for $f\colon \{0, 1, \dots m\} \to \{0, 1, \dots, n\}$. Dette uendelige diagrammet er mye større enn det som strengt tatt trengs for å bestemme gruppe-strukturen på A, og inneholder i dette tilfellet heller ikke noen ytterligere informasjon. Diagrammet er også spesielt i den forstand at $HA(n_+) = A^n$ er det kartesiske produktet av n kopier av $HA(1_+) = A$, for hver $n \geq 0$.

1.3. Ringer. La nå R være en ring. Addisjonen i R definerer en underliggende abelsk gruppe, så vi kan danne en regel HR som ovenfor, som bl.a. tar $\{0, 1, \dots, n\}$ til $HR(n_+) = R^n$.

Multiplikasjonen og enheten i R lar oss nå definere enda to tilordninger som:

(3) til hvert par av heltall $m, n \geq 0$ tilordner funksjonen
$$\mu(m_+, n_+)\colon R^m \times R^n \to R^{mn}$$
(μ for multiplikasjon) som tar m-tuplet $(a_1, \dots, a_m) \in HR(m_+) = R^m$ og n-tuplet $(b_1, \dots, b_n) \in HR(n_+) = R^n$ til mn-tuplet
$$(a_i b_j \mid i = 1, \dots, m, j = 1 \dots, n)$$

i $HR(mn_+) = R^{mn}$, leksikografisk ordnet, og
(4) til hvert heltall $n \geq 0$ tilordner funksjonen

$$\eta(n_+)\colon \{0, 1, \dots, n\} \to R^n$$

(η for enhet) som tar $i = 1, \dots, n$ til n-tuplet $(0, \dots, 1, \dots, 0)$ med 1 i i-te posisjon, og som tar 0 til $(0, \dots, 0)$.

Ring-multiplikasjonen kan rekonstrueres fra tilfellet $m = n = 1$, hvor avbildningen $\mu(1_+, 1_+)\colon R \times R \to R$ tar $a_1 \in R$ og $b_1 \in R$ til $a_1 b_1 \in R$. Enheten i ringen er bildet av 1 under $\eta(1_+)\colon \{0, 1\} \to R$. Igjen er samlingen av alle funksjonene $\mu(m_+, n_+)$ mye mer omfattende enn det som strengt tatt er nødvendig for å bestemme ring-strukturen på R.

1.4. $\mathbb{S}$-moduler. En fruktbar topologisk generalisering oppstår ved å erstatte mengdene A^n, R^n, etc. ovenfor med vilkårlige topologiske rom. La kort

$$n_+ = \{0, 1, \dots, n\}$$

for $n \geq 0$, med $0 \in n_+$ som basis-punkt.

Definisjon. En "vidunderlig ny abelsk gruppe", eller en $\mathbb{S}$-*modul*, er en regel E som:

(1) til hvert heltall $n \geq 0$ tilordner et topologisk rom $E(n_+)$, med et valgt basis-punkt $*$, og
(2) til hver funksjon $f\colon m_+ \to n_+$ med $f(0) = 0$ tilordner en kontinuerlig avbildning $E(f)\colon E(m_+) \to E(n_+)$, med $E(f)(*) = *$.

Vi forutsetter at $E(0_+) = *$, $E(g \circ f) = E(g) \circ E(f)$ og $E(id) = id$.

Vi kan tenke på en slik regel som diagrammet av alle rommene $E(n_+)$ for $n \geq 0$, knyttet sammen med alle avbildningene $E(f)$ for $f\colon m_+ \to n_+$. Nå er det typisk ikke slik at dette diagrammet er bestemt av noe endelig del-diagram.

1.5. $\mathbb{S}$-algebraer. En $\mathbb{S}$-algebra er en $\mathbb{S}$-modul med en passende multiplikasjon og enhet.

Definisjon. En "vidunderlig ny ring", eller en $\mathbb{S}$-*algebra*, er en $\mathbb{S}$-modul E utstyrt med:

(3) en kontinuerlig avbildning

$$\mu(m_+, n_+)\colon E(m_+) \times E(n_+) \to E(mn_+)$$

som tar punkter på formen $(e, *)$ eller $(*, e)$ til $*$, for hvert par av heltall $m, n \geq 0$, og
(4) en kontinuerlig avbildning

$$\eta(n_+)\colon n_+ \to E(n_+)$$

som tar $0 \in n_+$ til $*$, for hvert heltall $n \geq 0$.

Vi forutsetter at $\mu \circ (E(f) \times E(g)) = E(f \times g) \circ \mu$ (distributivitet, passende fortolket), at $\mu(\ell_+, \mu(m_+, n_+)) = \mu(\mu(\ell_+, m_+), n_+)$ (assosiativitet), og at $\mu(1_+, n_+) \circ (\eta(1_+) \times id) = id = \mu(n_+, 1_+) \circ (id \times \eta(1_+))$ (unitalitet).

1.6. Noen eksempler.

Eilenberg–Mac Lane spektra. Gitt en ring R kan vi oppfatte hver mengde R^n som et topologisk rom med den diskrete topologien, med basispunkt $* = (0, \dots, 0)$. Da er regelen HR et eksempel på en $\mathbb{S}$-algebra, som kalles *Eilenberg–Mac Lane spekteret* til R. Ringer i algebraisk forstand innlemmes derfor i klassen av vidunderlige nye ringer ved å ta R til HR.

$$\{\text{Ringer}\} \xrightarrow{H} \{\mathbb{S}\text{-algebraer}\}$$

Sfærespekteret. Det mest fundamentale eksempelet på en $\mathbb{S}$-algebra er *sfærespekteret* $\mathbb{S}$. Det er regelen som:

(1) til hvert heltall $n \geq 0$ tilordner mengden $\mathbb{S}(n_+) = n_+$ med den diskrete topologien og 0 som basispunkt, og
(2) tar en funksjon $f\colon m_+ \to n_+$ med $f(0) = 0$ til samme funksjon $\mathbb{S}(f)\colon m_+ \to n_+$ oppfattet som en kontinuerlig avbildning.

Dette er en $\mathbb{S}$-modul, som videre er utstyrt med

(3) multiplikasjonen
$$\mu(m_+, n_+)\colon m_+ \times n_+ \to mn_+$$
som identifiserer $\{1, \dots, m\} \times \{1, \dots n\}$ med $\{1, \dots, mn\}$ via den leksikografiske ordningen, og tar par på formen $(i, 0)$ eller $(0, j)$ til 0, og
(4) enheten
$$\eta(n_+)\colon n_+ \to n_+$$
som er lik identitetsavbildningen.

Topologisk K-teori. Et tredje eksempel på en $\mathbb{S}$-algebra heter ku, og representerer (konnektiv, kompleks) *topologisk K-teori*. Det har

$$ku(1_+) = \coprod_{d \geq 0} \mathrm{Gr}_d(\mathbb{C}^\infty)$$

der $\mathrm{Gr}_d(\mathbb{C}^\infty)$ er Grassmann–rommet av alle d-dimensjonale komplekse underrom i $\mathbb{C}^\infty$. Definisjonen av rommene $ku(n_+)$ for $n \geq 2$ er litt mer komplisert, men kan gjøres som i [Se74].

Det gir mening å snakke om avbildninger mellom $\mathbb{S}$-moduler (eller $\mathbb{S}$-algebraer), som generaliserer homomorfier mellom abelske grupper (eller ringer). Spesielt er det interessante avbildninger

$$\mathbb{S} \to ku \to H\mathbb{Z}\,.$$

1.7. Stabile ekvivalenser. Definisjonen ovenfor av en $\mathbb{S}$-modul (eller $\mathbb{S}$-algebra) er såpass fleksibel at det er naturlig å oppfatte visse par av $\mathbb{S}$-moduler (eller $\mathbb{S}$-algebraer) som ekvivalente. Det er litt teknisk å presisere dette, men vi håper følgende skisse er noenlunde forståelig.

En $\mathbb{S}$-modul E kan på en veldefinert måte utvides til en regel som:

(1) til hvert topologisk rom X med basispunkt 0 tilordner et topologisk rom $E(X)$ med basispunkt $*$, og
(2) til hver kontinuerlig avbildning $f\colon X \to Y$ med $f(0) = 0$ tilordner en kontinuerlig avbildning $E(f)\colon E(X) \to E(Y)$ med $E(f)(*) = *$, slik at $E(f)$ avhenger kontinuerlig av f.

For eksempel er utvidelsen av sfærespekteret $\mathbb{S}$ gitt ved $\mathbb{S}(X) = X$ for alle rom X. Vi vil nå evaluere den utvidede regelen E på de k-dimensjonale sfærene S^k (= enhetssfæren i $\mathbb{R}^{k+1}$) for $k \geq 0$, og får dermed frem en sekvens av topologiske rom $E(S^k)$ for $k \geq 0$.

Den i-te *homotopi-gruppen* til $E(S^k)$ er definert som mengden av homotopiklasser av baserte avbildninger $S^i \to E(S^k)$, og skrives $\pi_i(E(S^k))$. For et fast heltall n kan vi se på den $(n+k)$-te homotopi-gruppen til $E(S^k)$, for hver $k \geq 0$, og la $k \to \infty$. Den direkte grensen av disse gruppene er en abelsk gruppe:

$$\pi_n(E) = \operatorname*{colim}_{k\to\infty} \pi_{n+k}(E(S^k)) .$$

Dette er den *n-te (stabile) homotopigruppen* til E. Samlingen av grupper $\pi_n(E)$ for $n \in \mathbb{Z}$ skrives kort $\pi_*(E)$, og oppfattes som en gradert abelsk gruppe, med $\pi_n(E)$ i grad n. For eksempel er $\pi_n(HR)$ lik R for $n = 0$, og lik 0 for $n \neq 0$. Gruppene $\pi_n(\mathbb{S})$ kalles de *stabile homotopi-gruppene av sfærer*. De er endelige for $n > 0$, og $\pi_0(\mathbb{S}) \cong \mathbb{Z}$.

Definisjon. En avbildning $\phi\colon D \to E$ av $\mathbb{S}$-moduler (eller $\mathbb{S}$-algebraer) kalles en *stabil ekvivalens* dersom den induserte homomorfien $\pi_n(\phi)\colon \pi_n(D) \to \pi_n(E)$ er en isomorfi for alle heltall n. Da sier vi at D og E er *stabilt ekvivalente*, og skjelner som oftest ikke mellom D og E.

Stabilt ekvivalente $\mathbb{S}$-moduler D og E vil ha isomorfe homotopi-grupper $\pi_*(D)$ og $\pi_*(E)$, men omvendingen av dette gjelder generelt ikke, fordi det ikke behøver finnes noen avbildning $\phi\colon D \to E$ som induserer isomorfien $\pi_*(D) \cong \pi_*(E)$.

Dersom E er en $\mathbb{S}$-algebra gir multiplikasjonen μ og enheten η opphav til et produkt $\mu\colon \pi_m(E) \times \pi_n(E) \to \pi_{m+n}(E)$ og en enhet $\eta\colon \pi_n(\mathbb{S}) \to \pi_n(E)$, som gjør $\pi_*(E)$ til en gradert $\pi_*(\mathbb{S})$-algebra, og spesielt til en gradert ring. Vi kan derfor reflektere $\mathbb{S}$-algebraer tilbake til (graderte) ringer.

$$\{\mathbb{S}\text{-algebraer}\} \xrightarrow{\pi_*} \{\text{Graderte ringer}\}$$

Sammensetningen $\pi_* \circ H$ tar en ring til samme ring konsentrert i grad 0. I algebraiske anvendelser vil en $\mathbb{S}$-algebra E gjerne opptre i form av sine homotopigrupper $\pi_*(E)$.

2. Geometriske, fysiske og aritmetiske anvendelser

2.1. Algebraisk K-teori. La R være en ring, f.eks. ringen av algebraiske heltall i en tallkropp. Med "aritmetiske egenskaper" over R kan vi bl.a. tenke på informasjon om eksistens eller entydighet av primfaktoriseringer for tall i R. Dersom vi lar "tall i R" også omfatte "ideelle tall", dvs. idealer $I \subset R$, så eksisterer primfaktoriseringer i alle Noetherske ringer. Idealer er eksempler på moduler, og mange av de aritmetiske egenskapene til R er gjenspeilet i kategorien av alle endelig-genererte projektive R-moduler. *Algebraisk K-teori* knytter en $\mathbb{S}$-modul $K(R)$ til denne kategorien (som i [Se74]), og fanger opp mange av de aritmetiske egenskapene til R. For eksempel inneholder den projektive klasse-gruppen $\pi_0(K(R))$ obstruksjonene mot entydig primfaktorisering.

Mer generelt, la E være en $\mathbb{S}$-algebra. Algebraisk K-teori knytter fortsatt en $\mathbb{S}$-modul $K(E)$ til E. (Dersom E er kommutativ er $K(E)$ igjen en $\mathbb{S}$-algebra.) Ledet av det klassiske algebraiske tilfellet vil vi tenke på $K(E)$ som en bærer av aritmetisk informasjon om E. Det er interessant at slik "aritmetisk informasjon" kan ha helt andre inkarnasjoner i andre tilsynelatende uavhengige deler av matematikken !

Som nevnt i innledningen skal vi nå se på tre slike anvendelser, til henholdsvis geometrisk topologi, matematisk fysikk og tallteori.

2.2. Symmetrier av mangfoldigheter. Gitt en kompakt Riemannsk mangfoldighet M danner mengden av isometrier $M \to M$ en *Lie-gruppe*. Mer generelt kan man studere mengden av diffeomorfier $M \to M$, eller av homeomorfier $M \to M$. Disse danner (uendelig-dimensjonale) topologiske grupper $\mathrm{Diff}(M)$ og $\mathrm{Homeo}(M)$, som vi oppfatter som de *differensiable* og *topologiske symmetrigruppene* til M. Mye mindre er kjent om disse uendelig-dimensjonale symmetrigruppene enn om de klassiske endelig-dimensjonale Lie-gruppene.

Velg et basispunkt p i M. Det *baserte løkkerommet* ΩM er rommet av kontinuerlig parametriserte veier i M som begynner og slutter i p. Dette er en topologisk (semi-)gruppe under sammenføyning av veier. Da finnes det en $\mathbb{S}$-algebra $\mathbb{S}[\Omega M]$ som til hvert heltall n_+ tilordner det topologiske rommet

$$\mathbb{S}[\Omega M](n_+) = (\Omega M \times \{1, \dots, n\})_+ \,.$$

Multiplikasjonen μ på $\mathbb{S}[\Omega M]$ er avledet fra gruppeoperasjonen. Vi tenker på $\mathbb{S}[\Omega M]$ som *gruppe-ringen* til ΩM over $\mathbb{S}$, eventuelt som *gruppe-$\mathbb{S}$-algebraen* til ΩM.

Aritmetikken til $\mathbb{S}[\Omega M]$ gjenspeiles i dens algebraiske K-teori $K(\mathbb{S}[\Omega M])$, som Waldhausen kaller $A(M)$. Waldhausen's "stabile parametriserte h-kobordismeteorem" (ca. 1982) sier at man fra $A(M) = K(\mathbb{S}[\Omega M])$ kan lese av homotopi-typen til $\mathrm{Diff}(M)$ og $\mathrm{Homeo}(M)$, med voksende nøyaktighet ettersom dimensjonen til M vokser. Teoremet knytter altså en tett forbindelse mellom

- aritmetikk i gruppe-ringer over $\mathbb{S}$ for løkkeroms-grupper, og
- rom av differensiable og topologiske symmetrier av høy-dimensjonale mangfoldigheter.

2.3. Strenger og felt-teorier. I fysisk *streng-teori* modelleres partikler med lukkede kurver i et gitt rom M. Det *fri løkkerommet* ΛM er rommet av slike lukkede kurver. Tidsutviklingen til en enkelt slik partikkel er gitt ved en sylinderflate i M, eller en kurve i ΛM. Når partikler vekselvirker vil de tilhørende flatene forgrene seg, og er ikke lenger fullstendig representert ved kurver i ΛM. For å kvantisere dette bildet trengs et tilstandsrom for hver partikkel, som er et vektorrom for hver løkke i M, dvs. en vektorbunt over ΛM. Videre trengs en operator som viser tidsutviklingen av tilstanden, som er en lineær avbildning for hver flate i M, mellom passende tensorprodukter av vektorrommene assosiert til flatens randsirkler. Det er ikke så klart hvordan denne siste strukturen kan uttrykkes over ΛM, dels fordi det er relativistisk påkrevet at disse strukturene skal være lokalt definert over M.

Michael Atiyah [At88] og Segal [Se88a] har aksiomatisert ulike varianter av den ønskede strukturen, henholdsvis som *topologiske-* og *konforme felt-teorier*. Segal [Se88b] har videre etterlyst en teori for såkalte "elliptiske objekter" over M, som skal gi opphav til slike strukturer, dvs. slike felt-teorier.

En beregning av Christian Ausoni og Rognes [AR02] har ledet Nils Baas, Bjørn Dundas og Rognes til å studere aritmetikk i $\mathbb{S}$-algebraen ku som representerer topologisk K-teori. De aritmetiske egenskapene til ku bæres av $K(ku)$, dvs. algebraisk K-teori av topologisk K-teori, og det virker nå som at Segals elliptiske objekter er representert av $K(ku)$. Så en avbildning $M \to K(ku)$ gir et elliptisk objekt og en felt-teori over M.

Dersom dette fører frem er det altså en tett forbindelse mellom

- aritmetikk i topologisk K-teori ku, og
- elliptiske objekter og felt-teorier.

2.4. Modulære former og gittere. En mer direkte anvendelse av $\mathbb{S}$-algebraer (som ikke involverer modul-kategorier eller algebraisk K-teori) handler om en forfining av teorien for (elliptiske) modulære former, som skyldes Mike Hopkins og medarbeidere fra ca. 1995. Her gir vi et kort sammendrag, mens vi i kapittel 3 definerer de fleste begrepene og forklarer denne anvendelsen i mer detalj.

En modulær form forsøker å være en regulær funksjon på moduli-rommet av isomorfi-klasser av elliptiske kurver. For komplekse elliptiske kurver er de komplekse modulære formene $\mathcal{M}_*(\mathbb{C})$ særdeles symmetriske kompleks analytiske funksjoner definert på det øvre komplekse halvplanet, som studeres med analytiske metoder. For heltallige elliptiske kurver er de heltallige modulære formene $\mathcal{M}_*(\mathbb{Z})$ særdeles symmetriske polynomer, som studeres med aritmetiske- og algebro-geometriske metoder. Hopkins og Haynes Miller (ca. 1995) ga mening til *elliptiske $\mathbb{S}$-algebraer*, med en assosiert $\mathbb{S}$-algebra tmf av *topologiske modulære former*. Denne teorien bruker topologiske konstruksjoner med $\mathbb{S}$-algebraer på en helt essensiell måte.

Homotopigruppene $\pi_*(tmf) = \mathcal{M}_*(\mathbb{S})$ ble beregnet av Hopkins og Mark Mahowald (ca. 1994). Det er en ring-homomorfi fra topologiske modulære former til heltallige modulære former:

$$\pi_*(tmf) = \mathcal{M}_*(\mathbb{S}) \to \mathcal{M}_*(\mathbb{Z}) = \frac{\mathbb{Z}[c_4, c_6, \Delta]}{(1728\Delta = c_4^3 - c_6^2)}\,.$$

Den homotopiske graden (til venstre) er halvparten av den modulære vekten (til høyre). Multiplikasjon med 24 annihilerer både kjernen og kokjernen til denne avbildningen. Videre er kan ringen av heltallige modulære former inkluderes inn i ringen av komplekse modulære former:

$$\mathcal{M}_*(\mathbb{Z}) \to \mathcal{M}_*(\mathbb{C}) = \mathbb{C}[E_4, E_6]\,.$$

Den modulære vekten er den samme på begge sider.

Modulære former opptrer kanskje mest naturlig som theta-funksjoner til *jevne unimodulære gittere*. Richard E. Borcherds, som mottok Fields-medaljen i 1998 for sitt arbeid om "moonshine" formodningene (som knytter modulære former til endelige simple grupper, så som Fischer–Griess Monster-gruppen), viste i [Bo95] at ikke alle heltallige modulære former oppstår på denne måten, men at theta-funksjonene (og dermed deres heltallige lineær-kombinasjoner) oppfyller visse kongruenser. Hopkins innså at disse kongruensene nettopp beskriver bildet av $\mathcal{M}_*(\mathbb{S})$ i $\mathcal{M}_*(\mathbb{Z})$.

Teorem (Borcherds, Hopkins). *La L være et jevnt unimodulært gitter. Da er dets theta-funksjon $\theta_L \in \mathcal{M}_*(\mathbb{Z})$ topologisk, dvs. med i bildet av $\mathcal{M}_*(\mathbb{S}) \to \mathcal{M}_*(\mathbb{Z})$.*

Dette antyder at theta-funksjonen til et jevnt unimodulært gitter kan defineres som en topologisk modulær form, dvs. som et element i $\pi_*(tmf)$. (Forfatteren kjenner ingen slik direkte konstruksjon.)

$$\begin{tikzcd}
& \text{Jevne unimodulære gittere} \arrow[dl, dashed, "?"'] \arrow[d] \arrow[dr, "\theta"] & \\
\text{Topologiske modulære former} \arrow[r] & \text{Heltallige modulære former} \arrow[r] & \text{Komplekse modulære former}
\end{tikzcd}$$

2.5. Streng-mangfoldigheter og Witten-genus. Ed Witten, som mottok Fields-medaljen i 1990 for sine arbeider i matematisk fysikk, konstruerte i [Wi88] et "genus" som til en streng-mangfoldighet M (der strukturgruppen til normalbunten er løftet til den 3-sammenhengende overdekningen $O\langle 8\rangle$ av O) assosierer en heltallig modulær form $\Phi(M) \in \mathcal{M}_*(\mathbb{Z})$. Definisjonen er motivert av en tenkt Dirac-operator mellom spinor-bunter over det fri løkkerommet ΛM til en slik mangfoldighet, selv om dette ikke uten videre gir mening matematisk. Matthew Ando, Hopkins og Neil Strickland [AHS01] viser at dette Witten-genuset best kan realiseres som en avbildning av $\mathbb{S}$-algebraer

$$\Phi\colon MO\langle 8\rangle \to tmf\,.$$

Den induserte homomorfien

$$\pi_*(\Phi)\colon \Omega_*^{\text{string}} = \pi_*(MO\langle 8\rangle) \to \pi_*(tmf) = \mathcal{M}_*(\mathbb{S})$$

tar bordismeklassen til M til en topologisk modulær form, som har bilde $\Phi(M)$ i $\mathcal{M}_*(\mathbb{Z}) \subset \mathcal{M}_*(\mathbb{C})$.

Konstruksjonen av denne avbildningen Φ (i et parallelt komplekst tilfelle) involverer "kubiske strukturer" over elliptiske kurver, som eksisterer entydig ved Niels Henrik Abels teorem om divisorer på algebraiske kurver.

Ved Hopkins og Mahowalds beregninger er $\pi_*(\Phi)$ surjektiv. Det følger at theta-funksjonen til ethvert jevnt unimodulært gitter kan realiseres som Witten-genuset til en streng-mangfoldighet. Spesielt gjelder dette theta-funksjonen til Leech-gitteret Λ_{24}, og disse resultatene besvarer positivt Hirzebruchs "Prize Question" fra [HBJ92, s. 86].

3. Topologiske modulære former

En referanse for avsnittene 3.1–3.3 er [Si94, Ch. I].

3.1. Komplekse elliptiske kurver. Et *elliptisk integral* (f.eks. av første type) er en kompleks funksjon gitt på formen

$$z = z(w) = \int_0^w \frac{dt}{\sqrt{(1-k^2t^2)(1-t^2)}}\,,$$

der $w \in \mathbb{C}$, og er knyttet til buelengde på ellipser. Abel innså at det i stedet er bedre å studere den omvendte funksjonen $w = w(z)$, for $z \in \mathbb{C}$, som kalles en *elliptisk funksjon*. Denne er dobbelt-periodisk i $z \in \mathbb{C}$, så det finnes en fri abelsk gruppe (et *gitter*) $\mathbb{Z}\{\omega_1, \omega_2\} \subset \mathbb{C}$ slik at $w(z) = w(z + m\omega_1 + n\omega_2)$ for alle $m\omega_1 + n\omega_2 \in \mathbb{Z}\{\omega_1, \omega_2\}$. Dermed er kvotientgruppen

$$\mathbb{C}/\mathbb{Z}\{\omega_1, \omega_2\}$$

det naturlige definisjonsrommet for den elliptiske funksjonen $w(z)$. En slik kompleks kurve av genus 1 (en torus) kalles derfor en *elliptisk kurve*.

Vi kan anta at (ω_1, ω_2) er positivt orientert, så $\tau = \omega_2/\omega_1$ har positiv imaginærdel. Multiplikasjon med ω_1 er en isomorfi fra $\mathbb{C}/\mathbb{Z}\{1, \tau\}$ til $\mathbb{C}/\mathbb{Z}\{\omega_1, \omega_2\}$. La $\mathcal{H} = \{\tau \in \mathbb{C} \mid \operatorname{im} \tau > 0\}$ være det øvre komplekse halvplan. Enhver elliptisk kurve er altså isomorf med en på formen $\mathbb{C}/\mathbb{Z}\{1, \tau\}$, så funksjonen som tar $\tau \in \mathcal{H}$ til den elliptiske kurven $\mathbb{C}/\mathbb{Z}\{1, \tau\}$ parametriserer hele rommet av isomorfiklasser av elliptiske kurver; det såkalte (elliptiske) *moduli-rommet*. To parametere τ og τ' i $\mathcal{H}$ definerer isomorfe elliptiske kurver hvis og bare hvis τ' kan skrives som

$$\tau' = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \tau = \frac{a\tau + b}{c\tau + d}$$

for en matrise $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ i den *modulære gruppen* $SL_2(\mathbb{Z})$, der a, b, c, d er heltall slik at $ad - bc = 1$. Dermed kan moduli-rommet identifiseres med orbit-rommet $\mathcal{H}/SL_2(\mathbb{Z})$ for denne gruppevirkningen av $SL_2(\mathbb{Z})$ på $\mathcal{H}$.

3.2. Komplekse modulære former. Weierstraß $\wp$-funksjonen

$$\wp(z; \tau) = \frac{1}{z^2} + \sum_{m,n \in \mathbb{Z}} \left(\frac{1}{(m + n\tau - z)^2} - \frac{1}{(m + n\tau)^2} \right)$$

(der $(m, n) = (0, 0)$ utelates fra summen) er en elliptisk funksjon av z, med perioder 1 og τ, og er derfor naturlig definert som en funksjon av restklassen $[z] \in \mathbb{C}/\mathbb{Z}\{1, \tau\}$ til $z \in \mathbb{C}$. Den oppfyller differensiallikningen

$$\wp'(z; \tau)^2 = 4\wp(z; \tau)^3 - \frac{(2\pi)^4}{12} E_4(\tau)\wp(z; \tau) - \frac{(2\pi)^6}{216} E_6(\tau)$$

(derivasjon m.h.p. z), for visse kompleks analytiske funksjoner $E_4(\tau)$ og $E_6(\tau)$ som kalles *normaliserte Eisenstein-rekker*. Dermed definerer formelen

$$[z] \longmapsto (x, y) = ((2\pi)^2 \wp(z; \tau), (2\pi)^3 \wp'(z; \tau))$$

en isomorfi fra $\mathbb{C}/\mathbb{Z}\{1, \tau\}$ til den komplekse projektive kurven C_τ gitt ved den polynomielle likningen

$$C_\tau : y^2 = 4x^3 - \frac{E_4(\tau)}{12} x - \frac{E_6(\tau)}{216} \,,$$

dvs. tillukningen i $\mathbb{C}P^2 = P^2(\mathbb{C})$ av løsningene $(x, y) \in \mathbb{C}^2$ til denne likningen. (Vi har introdusert faktorene $(2\pi)^2$ og $(2\pi)^3$ i denne isomorfien for å eliminere noen tilsvarende transcendente skaleringsfaktorer i sammenlikningen mellom heltallige og komplekse modulære former i avsnitt 3.5 nedenfor.)

Merk at $E_4(\tau)$ og $E_6(\tau)$ er funksjoner fra rommet $\mathcal{H}$ som parametriserer elliptiske kurver. Hvis $\tau, \tau' \in \mathcal{H}$ parametriserer isomorfe elliptiske kurver $\mathbb{C}/\mathbb{Z}\{1, \tau\}$ og $\mathbb{C}/\mathbb{Z}\{1, \tau'\}$, dvs. representerer samme punkt i moduli-rommet, så er de komplekse kurvene C_τ og

$$C_{\tau'}\colon y^2 = 4x^3 - \frac{E_4(\tau')}{12}x - \frac{E_6(\tau')}{216}$$

isomorfe, som nesten er nok til å slutte at $E_4(\tau) = E_4(\tau')$ og $E_6(\tau) = E_6(\tau')$. Så $E_4(\tau)$ og $E_6(\tau)$ er nesten definert som funksjoner fra moduli-rommet. Det som er helt korrekt er at E_4 og E_6 er komplekse modulære former av vekt henholdsvis 4 og 6:

Definisjon. En *kompleks modulær form* f av vekt k er en kompleks analytisk funksjon definert på $\mathcal{H} \subset \mathbb{C}$, som er begrenset nær ∞i, slik at

$$f(\tau) = f(\tau + 1) \qquad \text{og} \qquad f(-1/\tau) = \tau^k f(\tau)\,.$$

Dette er ekvivalent med å kreve at

$$f(\frac{a\tau + b}{c\tau + d}) = (c\tau + d)^k f(\tau)$$

for alle $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ i $SL_2(\mathbb{Z})$, for de to matrisene $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ og $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ genererer hele $SL_2(\mathbb{Z})$.

Teorem. *La $\mathcal{M}_k(\mathbb{C})$ være vektorrommet av komplekse modulære former av vekt k, for alle heltall k. Da er $\mathcal{M}_*(\mathbb{C})$ en gradert $\mathbb{C}$-algebra, og*

$$\mathcal{M}_*(\mathbb{C}) \cong \mathbb{C}[E_4, E_6]$$

med E_4 i vekt 4 og E_6 i vekt 6.

3.3. Rekkeutviklinger. Det er en avbildning $\mathcal{H} \to \mathcal{D} = \{q \in \mathbb{C} \mid |q| < 1\}$ til den åpne enhets-disken i $\mathbb{C}$, gitt ved

$$\tau \longmapsto q = e^{2\pi i\tau}\,.$$

En kompleks modulær form f oppfyller $f(\tau) = f(\tau + 1)$ og er begrenset nær ∞i, og kan derfor oppfattes som en kompleks analytisk funksjon $f(q)$ av $q \in \mathcal{D}$. Vi kan rekkeutvikle denne som

$$f(q) = \sum_{n\geq 0} c_n q^n \quad \in \mathbb{C}[[q]]$$

for passende komplekse koeffisienter c_n. Her er $\mathbb{C}[[q]]$ ringen av formelle potensrekker i q med komplekse koeffisienter.

Disse *q-utviklingene* for E_4 og E_6 har faktisk heltallige koeffisienter:

$$E_4(q) = 1 + 240\sum_{n\geq 1} \sigma_3(n)q^n \quad \in \mathbb{Z}[[q]]$$

$$E_6(q) = 1 - 504\sum_{n\geq 1} \sigma_5(n)q^n \quad \in \mathbb{Z}[[q]]$$

der divisorpotenssummen $\sigma_k(n) = \sum_{d|n} d^k$ er et naturlig tall. *Diskriminanten* til C_τ er

$$\Delta = \frac{E_4^3 - E_6^2}{1728}$$

og har også heltallig q-utvikling (Jacobi):

$$\Delta = q \prod_{n\geq 1} (1-q^n)^{24} = q - 24q^2 + \dots \quad \in \mathbb{Z}[[q]]\,.$$

Vi kan derfor oppfatte $\mathcal{M}_*(\mathbb{C})$ som den komplekse underalgebraen av $\mathbb{C}[[q]]$ generert av $E_4, E_6 \in \mathbb{Z}[[q]] \subset \mathbb{C}[[q]]$. Den inneholder også $\Delta \in \mathbb{Z}[[q]]$, med $1728\Delta = E_4^3 - E_6^2$.

3.4. Theta-funksjoner. Et *gitter* L i $\mathbb{R}^m$ er en diskret undergruppe $L \subset \mathbb{R}^m$ slik at kvotientgruppen $\mathbb{R}^m/L$ er kompakt. Da er $L \cong \mathbb{Z}^m$, og vi kan velge m generatorer $\vec{b}_1, \dots, \vec{b}_m$ for L som danner en reell basis i $\mathbb{R}^m$. En vektor $\vec{x} \in L$ kan entydig skrives på formen

$$\vec{x} = v_1\vec{b}_1 + \dots + v_m\vec{b}_m$$

med $v_1, \dots, v_m$ hele tall, slik at $v = (v_1, \dots, v_m) \in \mathbb{Z}^m$ er koordinatene til $\vec{x}$ med hensyn på basisen $(\vec{b}_1, \dots, \vec{b}_m)$. Den Euklidiske kvadratnormen

$$\|\vec{x}\|^2 = x_1^2 + \dots\ x_m^2$$

for $\vec{x} = (x_1, \dots, x_m) \in \mathbb{R}^m$ restrikterer seg til en positivt definitt kvadratisk form på L, og dermed på $\mathbb{Z}^m$. Den siste kan skrives

$$Q(v) = \frac{1}{2} v^t A v = \frac{1}{2} \sum_{i,j=1}^{m} a_{ij} v_i v_j$$

for $v = (v_1, \dots, v_m) \in \mathbb{Z}^m$, der $A = (a_{ij})$ er en symmetrisk, positivt definitt $m \times m$ matrise. (Legg merke til faktoren 1/2 !)

Dersom A er *heltallig* (alle $a_{ij} \in \mathbb{Z}$) og *jevn* (diagonalelementene a_{ii} er partall), så er kvadratnormen til hvert element i L et heltall, dvs. den kvadratiske formen $Q(v)$ tar bare heltallige verdier. Dersom $\det(A) = 1$ sier vi videre at A er *unimodulær*.

Definisjon. Et *jevnt unimodulært gitter* av rang m er et gitter L i $\mathbb{R}^m$ slik at den tilhørende positivt definitte symmetriske matrisen A er heltallig, jevn og unimodulær.

Rangen m til et jevnt unimodulært gitter er alltid delelig med 8. Opp til isomorfi er det eneste eksempelet av rang 8 gitt ved matrisen

$$E_8\colon \begin{bmatrix} 2 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 \end{bmatrix}$$

som ble konstruert av A. Korkine og G. Zolotareff i [KZ73]. Ernst Witt viste i [Wi41] at det er nøyaktig to eksempler av rang 16, som kalles $2E_8$ og D_{16}^+. Hans-Volker Niemeier viste så i [Ni73] at det er nøyaktig 24 forskjellige jevne unimodulære gittere av rang 24, deriblant det særegne Leech-gitteret Λ_{24} som ble funnet av John Leech i [Le67]. Klassifikasjonen av jevne unimodulære gittere av høy rang regnes som utilgjengelig.

Definisjon. *Theta-funksjonen* $\theta_L(q) \in \mathbb{Z}[[q]]$ til et jevnt gitter L er definert ved q-rekken

$$\theta_L(q) = \sum_{v \in \mathbb{Z}^m} q^{Q(v)} = \sum_{n \geq 0} c_n q^n \,,$$

der c_n er antallet vektorer i L med kvadratnorm lik n.

Theta-funksjonen husker altså kvadratnormen til alle vektorene i gitteret. Et enkelt eksempel er gitteret $L = \mathbb{Z}$ i $\mathbb{R}$, med $m = 1$ og $Q(v) = v^2$ for $v \in \mathbb{Z}$, som er representert av den jevne matrisen $A = [2]$ (som ikke er unimodulær). Dets theta-funksjon er

$$\theta_{\mathbb{Z}}(q) = \sum_{v \in \mathbb{Z}} q^{v^2} = 1 + 2q + 2q^4 + 2q^9 + \dots .$$

Vi oppfatter θ_L som en kompleks analytisk funksjon av $\tau \in \mathcal{H}$ ved substitusjonen $q = e^{2\pi i \tau}$. Tilordningen $L \mapsto \theta_L$ avbilder mengden av jevne unimodulære gittere til mengden av modulære former, ved følgende klassiske resultat.

Teorem (Jacobi). *La L være et jevnt unimodulært gitter av rang m. Da er theta-funksjonen θ_L en kompleks modulær form av vekt $m/2$.*

For eksempel er $\theta_{E_8} = E_4$ i $\mathcal{M}_4(\mathbb{C})$, for dette er den eneste modulære formen av vekt 4 med konstantledd $c_0 = 1$ i q-utviklingen. Tilsvarende er $\theta_{2E_8} = \theta_{D_{16}^+} = E_4^2$ i $\mathcal{M}_8(\mathbb{C})$.

Når L gjennomløper de 24 jevne unimodulære Niemeier-gitterene av rank 24 (Λ_{24}, ... , D_{24}^+), så har den tilhørende theta-funksjonen θ_L formen $1 + c_1 q + \dots$, der c_1 (antallet vektorer av kvadratnorm lik 1) tar følgende verdier:

$$0, 48, 72, 96, 120, 144, 144, 168, 192, 216, 240, 240,$$
$$288, 288, 312, 336, 384, 432, 432, 528, 600, 720, 720, 1104 .$$

Se Conway og Sloane [CS, s. 407]. Merk at alle disse tallene er delelige med 24. Undergruppen av $\mathcal{M}_{12}(\mathbb{C})$ generert av theta-funksjonene θ_L er derfor lik den fri abelske gruppen $\mathbb{Z}\{E_4^3, 24\Delta\}$. Spesielt er diskriminanten Δ ikke selv en heltallig lineær-kombinasjon av slike theta-funksjoner.

Spørsmål. *Hvilke modulære former opptrer som theta-funksjoner av jevne unimodulære gittere ?*

Borcherds viste i [Bo95] at theta-funksjoner av jevne unimodulære gittere alltid oppfyller visse kongruenser, også i høyere rang.

Teorem (Borcherds). *La L være et jevnt unimodulært gitter av rang $m = 24k$. Da er konstantleddet c_0 i kvotienten*

$$\frac{\theta_L(q)}{\Delta^k} = q^{-k} + \cdots + c_0 + c_1 q + \ldots \qquad \in \mathbb{Z}[[q]]$$

alltid delelig med 24.

Dette resultatet kan i en viss forstand forklares av de topologiske modulære formene $\mathcal{M}_*(\mathbb{S})$. For å motivere definisjonen av disse må vi først se litt på de heltallige modulære formene $\mathcal{M}_*(\mathbb{Z})$.

3.5. Algebraiske elliptiske kurver. La R være en kommutativ ring. En *generalisert elliptisk kurve* definert over R er ("lokalt over $\mathrm{Spec}(R)$") gitt ved en likning

$$C\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

der $a_1, \ldots, a_4, a_6 \in R$. (Se f.eks. [AHS, §1].) Vi definerer heltallige polynomer

$$c_4 = (a_1^2 + 4a_2)^2 - 24(2a_4 + a_1a_3)$$
$$c_6 = -(a_1^2 + 4a_2)^3 + 36(a_1^2 + 4a_2)(2a_4 + a_1a_3) - 216(a_3^2 + 4a_6)$$

i ringen $A = \mathbb{Z}[a_1, \ldots, a_4, a_6]$, og finner at *diskriminanten*

$$\Delta = \frac{c_4^3 - c_6^2}{1728}$$

også er et heltallig polynom i $a_1, \ldots, a_4, a_6$. Ringen A er gradert ved at hver a_i har vekt i, slik at hver c_i har vekt i og Δ har vekt 12. Hvis x gis vekt 2 og y gis vekt 3 er likningen som definerer C homogen av vekt 6. (Se Silverman [Si86, Ch. III].)

Gitt verdier for $a_1, \ldots, a_4, a_6$ i R tar også hver c_i og Δ verdier i R. Den projektive algebraiske kurven C definert over R er en elliptisk kurve (glatt av genus 1) når diskriminanten Δ er invertibel i R.

To generaliserte elliptiske kurver C og C' definert over R er *strikt isomorfe* over R dersom C' fremkommer fra C ved et strikt affint koordinatskifte i (x, y)-planet på formen:

$$\begin{cases} x' = x + r \\ y' = sx + y + t \end{cases}$$

med r, s, t i R. De to projektive kurvene C og C' er da abstrakt isomorfe.

3.6. Heltallige modulære former. Regulære funksjoner fra moduli-rommet av strikte isomorfi-klasser av elliptiske kurver tar nå følgende form.

Definisjon. Betrakt par (R, C) der R er en kommutativ ring og C er en generalisert elliptisk kurve definert over R. En *heltallig modulær form* f er en regel som til hvert par (R, C) tilordner et element $f(R, C) \in R$, slik at

(1) $f(R, C) = f(R, C')$ dersom C og C' er strikt isomorfe over R, og
(2) $\phi(f(R, C)) = f(R', C')$ dersom $\phi\colon R \to R'$ er en ring-homomorfi og $C' = \phi_*(C)$ er kurven med koeffisienter $a_i' = \phi(a_i) \in R'$.

La $\mathcal{M}_*(\mathbb{Z})$ være mengden av heltallige modulære former.

La den generaliserte elliptiske kurven C være definert over polynomringen $A = \mathbb{Z}[a_1, \ldots, a_4, a_6]$, som gitt i avsnitt 3.5. Funksjonen $\mathcal{M}_*(\mathbb{Z}) \to A$ som tar $f \in \mathcal{M}_*(\mathbb{Z})$ til verdien $f(A, C) \in A$ er injektiv, og identifiserer $M_*(\mathbb{Z})$ med en under-ring av A. Et polynom i A tilhører $M_*(\mathbb{Z})$ hvis og bare hvis det er invariant under alle strikt affine koordinatskifter.

Følgende beregning skyldes John Tate og Pierre Deligne.

Teorem ([De75])**.** *Ringen av heltallige modulære former er den graderte ringen*

$$\mathcal{M}_*(\mathbb{Z}) \cong \frac{\mathbb{Z}[c_4, c_6, \Delta]}{(1728\Delta = c_4^3 - c_6^2)}$$

med c_4 i vekt 4, c_6 i vekt 6 og Δ i vekt 12.

En ekvivalent kategorisk definisjon er som følger: Dann kategorien med objekter alle par (R, C) med R en kommutativ ring og C en generalisert elliptisk kurve over R, og morfismer $(R, C) \to (R', C')$ gitt ved en ring-homomorfi $\phi\colon R \to R'$ og en strikt isomorfi $\phi_*(C) \cong C'$. Tilordningen $(R, C) \mapsto R$ definerer en funktor til kategorien av kommutative ringer. La ringen $\mathcal{M}_*(\mathbb{Z})$ være den inverse grensen av denne funktoren:

$$\mathcal{M}_*(\mathbb{Z}) = \lim_{(R,C)} R\,.$$

Denne funktoren har også høy(e)re deriverte funktorer, som ikke tidligere synes å ha blitt studert algebraisk, men som ble beregnet av Hopkins og Mahowald (ca. 1994). De danner E_2-leddet i en spektralsekvens som konvergerer til de topologiske modulære formene $\pi_*(tmf)$. Differensialene i denne spektralsekvensen er bestemt av topologien i konstruksjonen, og kan ikke uttrykkes rent algebraisk.

I det komplekse tilfellet ($R = \mathbb{C}$) svarer den analytiske elliptiske kurven $\mathbb{C}/\mathbb{Z}\{1, \tau\}$ til den algebraiske elliptiske kurven C_τ. Denne kan skrives som kurven C ovenfor med $a_1 = a_2 = a_3 = 0$, $a_4 = -E_4(\tau)/48$ og $a_6 = -E_6(\tau)/864$. Det følger at c_4, c_6 og Δ presis svarer til henholdsvis $E_4(q)$, $E_6(q)$ og Δ.

Altså kan de algebraiske modulære formene i $\mathcal{M}_*(\mathbb{Z})$ oppfattes som analytiske modulære former i $\mathcal{M}_*(\mathbb{C})$, via avbildningen som tar c_4, c_6 og Δ til henholdsvis E_4, E_6 og Δ:

$$\begin{tikzcd}
\mathcal{M}_*(\mathbb{Z}) \arrow[r] \arrow[d] & \mathcal{M}_*(\mathbb{C}) \arrow[d] \\
\mathbb{Z}[[q]] \arrow[r] & \mathbb{C}[[q]]
\end{tikzcd}$$

Spesielt har de heltallige modulære formene heltallige q-utviklinger.

3.7. Topologiske modulære former. En kommutativ $\mathbb{S}$-algebra E kalles *jevn* dersom den graderte ringen $\pi_*(E)$ inneholder en enhet $u \in \pi_2(E)$, og $\pi_1(E) = 0$. Da er $\pi_*(E) \cong \pi_0(E)[u, u^{-1}]$ konsentrert i jevne grader, og er 2-periodisk.

En jevn kommutativ $\mathbb{S}$-algebra E har en assosiert (1-dimensjonal kommutativ) *formell gruppe* P_E definert over $\pi_0(E)$. (Se Adams [Ad74, Part II].) En generalisert elliptisk kurve C over $\pi_0(E)$ er spesielt en algebraisk gruppe, og har en formell komplettering $\hat{C}$ som igjen er en (1-dimensjonal kommutativ) formell gruppe definert over $\pi_0(E)$. (Se Silverman [Si86, Ch. IV].)

Følgende definisjon skyldes Hopkins og Miller, og finnes i [AHS, §1].

Definisjon. En *elliptisk $\mathbb{S}$-algebra* er et trippel (E, C, t), der

(1) E er en jevn kommutativ $\mathbb{S}$-algebra,
(2) C er en generalisert elliptisk kurve over $\pi_0(E)$, og
(3) $t\colon P_E \to \hat{C}$ er en isomorfi av formelle grupper.

En *avbildning* $f\colon (E, C, t) \to (E', C', t')$ av elliptiske $\mathbb{S}$-algebraer er en $\mathbb{S}$-algebra homomorfi $f\colon E \to E'$ sammen med en isomorfi av elliptiske kurver $C' \to \pi_0(f)_*(C)$, som utvider den induserte avbildningen $\pi_0(f)_*(t) \circ (t')^{-1}\colon \hat{C}' \to \pi_0(f)_*(\hat{C})$.

Tilordningen $(E, C, t) \mapsto E$ definerer en funktor fra kategorien av elliptiske spektra til kategorien av kommutative $\mathbb{S}$-algebraer. La $\mathbb{S}$-algebraen tmf av *topologiske modulære former* være den inverse homotopi-grensen av denne funktoren:

$$tmf = \operatorname*{holim}_{(E,C,t)} E\,.$$

Avbildningen fra $\mathcal{M}_*(\mathbb{S}) = \pi_*(tmf)$ til $\mathcal{M}_*(\mathbb{C})$ kan sees som følger ([AHS, §1]). Til hver kompleks elliptisk kurve $\mathbb{C}/\mathbb{Z}\{1, \tau\}$ la $R_\tau = \mathbb{C}[u_\tau, u_\tau^{-1}]$ være en gradert ring med u_τ i grad 2, og la $E_\tau = HR_\tau$ være Eilenberg–Mac Lane $\mathbb{S}$-algebraen med $\pi_*(E_\tau) = R_\tau$. Den formelle gruppen P_{E_τ} er i dette tilfellet den additive formelle gruppen over $\mathbb{C}$, og projeksjonen $\mathbb{C} \to \mathbb{C}/\mathbb{Z}\{1, \tau\}$ induserer en isomorfi $t_\tau\colon P_{E_\tau} \to \hat{C}_\tau$. Tilordningen

$$(\mathbb{C}, \mathbb{C}/\mathbb{Z}\{1, \tau\}) \longmapsto (E_\tau, \mathbb{C}/\mathbb{Z}\{1, \tau\}, t_\tau)$$

embedder kategorien av komplekse elliptiske kurver fra avsnitt 3.6 inn som en underkategori av kategorien av elliptiske $\mathbb{S}$-algebraer.

Definisjonen av en "invers homotopi-grense" sikrer at det er en kanonisk ringhomomorfi

$$\mathcal{M}_*(\mathbb{S}) = \pi_*(\operatorname*{holim}_{(E,C,t)} E) \to \lim_{(E,C,t)} \pi_*(E)\,.$$

Restriksjon til underkategorien av komplekse elliptiske kurver gir en videre homomorfi

$$\lim_{(E,C,t)} \pi_*(E) \to \lim_{(\mathbb{C},\mathbb{C}/\{1,\tau\})} \mathbb{C}[u_\tau, u_\tau^{-1}] \cong \mathcal{M}_*(\mathbb{C})\,.$$

Den siste isomorfien identifiserer en kompleks modulær form $f(\tau) \in \mathcal{M}_*(\mathbb{C})$ av vekt k med elementet i den inverse grensen som tar verdien $f(\tau) \cdot u_\tau^k \in \mathbb{C}[u_\tau, u_\tau^{-1}]$ ved objektet $(\mathbb{C}, \mathbb{C}/\{1, \tau\})$.

Sammensetningen av disse avbildningene er ring-homomorfien $\mathcal{M}_*(\mathbb{S}) \to \mathcal{M}_*(\mathbb{C})$, som faktoriserer gjennom $\mathcal{M}_*(\mathbb{Z})$. Borcherds og Hopkins' teorem i avsnitt 2.4 følger nå ved å sammenlikne Hopkins og Mahowalds beregning av $\mathcal{M}_*(\mathbb{S})$ med Borcherds' teorem i avsnitt 3.4.

Referanser

[Ad74] J. Frank Adams, *Stable Homotopy and Generalised Homology*, Chicago Lectures in Mathematics, The University of Chicago Press, Chicago and London, 1974.

[AHS01] Matthew Ando, Michael J. Hopkins and Neil P. Strickland, *Elliptic spectra, the Witten genus and the theorem of the cube*, Invent. Math. **146** (2001), 595–687.

[At88] Michael Atiyah, *Topological quantum field theories*, Publ. Math., Inst. Hautes Étud. Sci. **68** (1988), 175–186.

[AR02] Christian Ausoni and John Rognes, *Algebraic K-theory of topological K-theory*, Acta Math. (2002) (to appear).

[Bo95] Richard E. Borcherds, *Automorphic forms on* $O_{s+2,2}(\mathbb{R})$ *and infinite products*, Invent. Math. **120** (1995), 161–213.

[Da70] Brian Day, *On closed categories of functors*, Reports of the Midwest Category Seminar, IV, Lecture Notes in Mathematics, vol. 137, Springer, Berlin, 1970, pp. 1–38.

[De75] Pierre Deligne, *Courbes elliptiques: formulaire d'après J. Tate*, Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Lecture Notes in Math., vol. 476, Springer, Berlin, 1975, pp. 53–73.

[EKMM97] Tony D. Elmendorf, Igor Kriz, Mike A. Mandell and J. Peter May, *Rings, modules, and algebras in stable homotopy theory. With an appendix by Mike Cole*, Mathematical Surveys and Monographs, vol. 47, American Mathematical Society, Providence, RI, 1997.

[HBJ] Friedrich Hirzebruch, Thomas Berger and Rainer Jung, *Manifolds and modular forms*; Translated by Peter S. Landweber, Aspects of Mathematics, vol. E 20, Friedr. Vieweg, Wiesbaden, 1992.

[HSS00] Mark Hovey, Brooke Shipley and Jeff Smith, *Symmetric spectra*, J. Am. Math. Soc. 13, 149–208 yr 2000.

[KZ73] A. Korkine and G. Zolotareff, *Sur les formes quadratiques*, Math. Ann. **6** (1873), 366–389.

[Le67] John Leech, *Notes on sphere packings*, Can. J. Math. **19** (1967), 251–267.

[Ly99] Manos Lydakis, *Smash products and* Γ*-spaces*, Math. Proc. Camb. Philos. Soc. **126** (1999), 311–328.

[Ni73] Hans-Volker Niemeier, *Definite quadratische Formen der Dimension* 24 *und Diskriminante* 1, J. Number Theory **5** (1973), 142–178.

[Se74] Graeme Segal, *Categories and cohomology theories*, Topology **13** (1974), 293–312.

[Se88a] ———, *The definition of conformal field theory*, Differential geometrical methods in theoretical physics (Proc. 16th Int. Conf., NATO Adv. Res. Workshop, Como/Italy 1987), NATO ASI Ser., Ser. C, vol. 250, 1988, pp. 165–171.

[Se88b] ———, *Elliptic cohomology* [*after Landweber–Stong, Ochanine, Witten, and others*], Sémin. Bourbaki, 40ème Année, Vol. 1987/88, Exp. No. 695, Astérisque **161–162** (1988), 187-201.

[Si86] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, 1986.

[Si94] ———, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, 1994.

[Wi41] Ernst Witt, *Eine Identität zwischen Modulformeln zweiten Grades*, Abhand. Math. Sem. Hamb. **14** (1941), 323–337.

[Wi88] Edward Witten, *The index of the Dirac operator in loop space*, Elliptic curves and modular forms in algebraic topology (Princeton, NJ, 1986), Lecture Notes in Math., vol. 1326, Springer, Berlin, 1988, pp. 161–181.

Matematisk institutt, Universitetet i Oslo
E-mail address: `rognes@math.uio.no`